					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P26S					Dokumenttitel: **Politik for tredjeparts- og leverandørsikkerhed**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard/forordning	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Clause 8	Operationelle kontroller for relationer med tredjeparter og leverandører
ISO/IEC 27002:2022	Controls 5.19–5.22	Sikkerhedskontroller for leverandører, kontraktuelle sikkerhedsvilkår, ændringsstyring, overvågning og gennemgang
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Anskaffelse, konfiguration, sammenkoblingsaftaler og kontroller for eksternt personale
EU GDPR	Articles 28, 32	Databehandleraftaler og sikkerhedskrav til databehandlere
EU NIS2	Articles 21(2)(a)(b)(i), 23(1)	Risikostyring i forsyningskæden og tilsyn med tredjepartstjenester
EU DORA	Articles 5(1)(2), 28(1)(2)	Styring af IKT-risici ved tredjepartsleverandører
COBIT 2019	APO10, APO12, DSS05	Leverandørstyring og integration af risici

1. Formål

1.1 Denne politik fastsætter de obligatoriske sikkerhedskrav for etablering, styring og ophør af relationer med tredjeparter og leverandører, som har adgang til eller påvirker organisationens data, systemer eller tjenester.

1.2 Den sikrer, at eksterne leverandører, herunder IT-supportleverandører, cloudtjenesteudbydere, softwareudviklere og leverandører af forretningsprocesser, håndterer virksomhedens aktiver sikkert og i overensstemmelse med gældende lovgivning og standarder.

1.3 Denne politik reducerer risici såsom datalækage, uautoriserede systemændringer, regulatoriske sanktioner eller driftsafbrydelser som følge af usikre eller utilstrækkeligt styrede tredjepartsforhold.

2. Omfang

2.1 Denne politik gælder for alle tredjeparter, der:

2.1.1 Leverer software, infrastruktur, hosting eller cloudtjenester

2.1.2 Har adgang til eller administrerer interne systemer, enheder eller applikationer

2.1.3 Håndterer virksomhedens data, dokumenter eller sikkerhedskopier

2.1.4 Understøtter forretningsdrift, HR, økonomi eller kundeservice

2.2 Den gælder også for:

2.2.1 Interne medarbejdere, der deltager i udvælgelse, engagement eller tilsyn med leverandører

2.2.2 Alt personale, der håndterer leverandøronboarding, kontrakter, adgang eller gennemgange

2.2.3 Ethvert system eller enhver proces, der er afhængig af tredjepartskomponenter eller tredjepartstjenester

3. Mål

3.1 Sikre, at alle leverandører opfylder klart definerede sikkerhedskrav.

3.2 Kræve, at leverandørkontrakter indeholder håndhævelige forpligtelser vedrørende sikkerhed, databeskyttelse og hændelseshåndtering.

3.3 Vurdere og dokumentere leverandørrisici, før aftaler underskrives, eller adgang tildeles.

3.4 Gennemføre regelmæssige gennemgange af højrisiko- eller kritiske leverandører for at bekræfte efterlevelse.

3.5 Etablere en formel proces for undtagelser, hændelseshåndtering og opdatering af kontrakter.

3.6 Understøtte efterlevelse af krav i ISO/IEC 27001:2022, GDPR, NIS2 og DORA vedrørende leverandørstyring.

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Har det overordnede ansvar for udvælgelse af leverandører og sikkerhedsmæssig efterlevelse

4.1.2 Godkender kontrakter, undtagelser og eskaleringer vedrørende leverandører

4.1.3 Fører tilsyn med hændelseshåndtering og beslutningstagning, når leverandører ikke opfylder deres forpligtelser

4.2 IT-leverandør eller intern sikkerhedskontakt

4.2.1 Vurderer den tekniske adgang, som leverandører anmoder om

4.2.2 Implementerer adgangsstyringsregler, gennemgår logfiler og verificerer sikker datahåndtering

4.2.3 Gennemgår dokumentation for sikkerhedskontroller, certificeringer eller revisionsresultater, hvor det er relevant

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Denne politik skal gennemgås mindst én gang årligt af direktøren med deltagelse af IT-leverandøren eller den leverandøransvarlige.

9.2 Politikken skal også gennemgås:

9.2.1 Efter enhver væsentlig ændring i juridiske, regulatoriske eller kontraktlige forpligtelser

9.2.2 Efter en leverandørrelateret sikkerhedshændelse eller en revisionskonstatering

9.2.3 Ved indførelse af nye leverandørkategorier (f.eks. kritiske SaaS-platforme)

9.3 Alle opdateringer skal være:

9.3.1 Dokumenteret med versionshistorik og begrundelse

9.3.2 Godkendt af direktøren

9.3.3 Kommunikeret til relevante interne medarbejdere og leverandøransvarlige

9.3.4 Opbevaret sammen med tidligere versioner i henhold til P14S – Dataopbevarings- og bortskaffelsespolitik

10. Relaterede politikker og sammenhænge

10.1 Effektiviteten af denne politik afhænger af koordinering med følgende SME-politikker for informationssikkerhed:

10.1.1 P2S – Politik for styringsroller og ansvarsområder: Tildeler ansvar for leverandørtilsyn og håndhævelse af kontrakter.

10.1.2 P4S – Politik for adgangskontrol: Indeholder regler for adgangsbegrænsning, som skal anvendes, når leverandører får systemadgang.

10.1.3 P17S – Databeskyttelses- og privatlivspolitik: Sikrer, at leverandører, der håndterer personoplysninger, efterlever databeskyttelsesprincipper og juridiske krav.

10.1.4 P14S – Dataopbevarings- og bortskaffelsespolitik: Gælder for alle data eller registreringer, der deles med eller opbevares af leverandører, og regulerer sikker bortskaffelse efter kontraktophør.

10.1.5 P30S – Politik for hændelseshåndtering: Definerer, hvordan der skal reageres, når en leverandør forårsager eller er involveret i en sikkerhedshændelse, herunder eskalering og procedurer for håndtering af bevismateriale.

10.2 Disse politikker skal fungere samlet for at sikre, at leverandørrisici styres gennem hele kontraktens livscyklus.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Kræver implementering af operationelle kontroller, herunder kontroller anvendt på relationer med tredjeparter og leverandører.

11.2 ISO/IEC 27002

11.2.1 Control 5.19 – Sikrer, at leverandørers sikkerhedsforanstaltninger er afstemt med organisationens krav.

11.2.2 Control 5.20 – Kræver formelle aftaler, der dækker sikkerhedsvilkår, ansvar og forpligtelser ved brud.

11.2.3 Control 5.21 – Styrer ændringer i leverandørtjenester, der kan påvirke sikkerhedstilstanden.

11.2.4 Control 5.22 – Kræver overvågning og gennemgang af leverandørtjenester og efterlevelse.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Regulerer anskaffelse af eksterne systemer og tjenester og kræver risikovurderinger og klart definerede forventninger.

11.3.2 SA-10 – Styrer konfigurations- og ændringsprocedurer vedrørende systemer, som administreres af tredjeparter.

11.3.3 CA-3 – Kræver sammenkoblingsaftaler for systemer, der involverer eksterne enheder.

11.3.4 PS-7 – Specificerer screening og ansvarlighed for eksternt personale.

11.4 EU GDPR (2016/679)

11.4.1 Article 28 – Kræver databehandleraftaler med leverandører, der fungerer som databehandlere.

11.4.2 Article 32 – Pålægger alle databehandlere at etablere passende tekniske og organisatoriske sikkerhedsforanstaltninger.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(a), (b), (i) – Pålægger styring af IKT-risici i forsyningskæden og kontroller for tredjeparter.

11.5.2 Article 23(1) – Kræver dokumenteret tilsyn med tredjepartstjenester for væsentlige og vigtige enheder.

11.6 EU DORA (2022/2554)

11.6.1 Article 5(1) – Kræver en styringsramme for IKT-risici, der omfatter alle kritiske tredjepartsudbydere.

11.6.2 Article 5(2) – Fastsætter kontraktuelle og operationelle kontroller for afhængigheder af IKT-tjenester.

11.6.3 Article 28(1), (2) – Etablerer regler for tilsyn med IKT-risici fra tredjeparter i den finansielle sektor.

11.7 COBIT 2019

11.7.1 APO10 – “Manage Suppliers” beskriver kontroller for sourcing og forventninger til styring af leverandørrelationer.

11.7.2 APO12 – “Manage Risk” integrerer leverandørrisici i organisationens risikostyring.

11.7.3 DSS05 – “Manage Security Services” gælder for administrerede tredjepartsleverandører og outsourcede tjenesteudbydere.